CLAIMS

We claim:

1. A method for over-the-air (OTA) activation of a wireless unit in a particular communications system, comprising:

A. causing the wireless unit to include a stored key, the stored key having been generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm;

B. causing the wireless unit to receive the wireless unit parameters and a verification number over-the-air, the wireless unit parameters including an identification of the particular communications system,

i. the verification number having been generated by using an authorization algorithm (A-algorithm) having the wireless unit parameters and a key as A-algorithm inputs, and

ii. the key having been generated by the K-algorithm having the identifier associated with the wireless unit as the K-algorithm input;

C. in response to receipt of the wireless unit parameters and the verification number, causing the wireless unit to generate a trial verification number by using the A-algorithm with the wireless unit parameters and the stored key as trial inputs;

D. causing the wireless unit to compare the verification number to the trial verification number for a match; and

E. in response to finding the match, causing the wireless unit to use the wireless unit parameters for activation of the wireless unit in the particular communications system.

2. The method of Claim 1, further comprising:

F. in response to failing to find the match, causing the wireless unit to fail to use the wireless unit parameters for the activation of the wireless unit in the particular communications system.

3. The method of Claim 1, wherein the wireless unit parameters comprise numeric assignment module (NAM) parameters.

4. The method of Claim 1, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

5. A method to prevent a wireless unit from being programmed over-the-air (OTA), comprising:

A. causing the wireless unit to include a stored key, the stored key being generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm;

B. causing the wireless unit, in response to receipt of information transmitted OTA to the wireless unit, to generate a trial verification number by using an authorization algorithm (A-algorithm) with the stored key and the information as A-algorithm inputs to the A-algorithm;

C. causing the wireless unit to compare the trial verification number with at least a portion of the information for a match; and

D. causing the wireless unit, in response to failing to find the match, to block programming of the wireless unit.

6. The method of Claim 5, wherein the information transmitted OTA to the wireless unit comprises numeric assignment module (NAM) parameters.

7. The method of Claim 5, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

8. The method of Claim 5, wherein the programming of the wireless unit comprises activation of the wireless unit in a particular communications system; and wherein causing the wireless unit to block the programming of the wireless unit comprises causing the wireless unit to block the activation of the wireless unit in the particular communications system.

9. A method for secure over-the-air (OTA) programming of a wireless unit, comprising:

A. causing the wireless unit to include a stored key;

B. causing the wireless unit to receive OTA wireless unit parameters and a verification number;

C in response to receipt of the wireless unit parameters and the verification number, causing the wireless unit to generate a trial verification number;

D. causing the wireless unit to compare the verification number to the trial verification number for a match; and

E. in response to finding the match, causing the wireless unit to use the wireless unit parameters for programming of the wireless unit.

10. The method of Claim 9, further comprising:

F. in response to failing to find the match, causing the wireless unit to block the programming of the wireless unit.

11. The method of Claim 9, wherein action A comprises causing the wireless unit to include the stored key, the stored key having been generated by using a key algorithm (K-algorithm) and having an identifier associated with the wireless unit as a K-algorithm input.

12. The method of Claim 11, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

13. The method of Claim 9, wherein the stored key is relatively unique to the wireless unit.

14. The method of Claim 9, wherein action B comprises causing the wireless unit to receive OTA the wireless unit parameters and the verification number, the verification number having been generated by an authorization algorithm (A-algorithm) having the wireless unit parameters and a key as A-algorithm inputs.

15. The method of Claim 14, wherein the key has been generated by a key algorithm (K-algorithm) having an identifier associated with the wireless unit as a K-algorithm input.

16. The method of Claim 14, wherein the key is relatively unique to the wireless unit.

17. The method of Claim 9, wherein action C comprises, in response to receipt of the wireless unit parameters and the verification number, causing the wireless unit to generate the trial verification number by using the wireless unit parameters and the stored key.

18. The method of Claim 17, wherein action C comprises, in response to receipt of the wireless unit parameters and the verification number, causing the wireless unit to generate the trial verification number by using an authorization algorithm (A-algorithm) with the wireless unit parameters and the stored key as A-algorithm inputs.

19. The method of Claim 9, wherein the wireless unit parameters comprise numeric assignment module (NAM) parameters.

20. The method of Claim 9, wherein the programming of the wireless unit comprises activation of the wireless unit in a particular communications system; and wherein causing the wireless unit to use the wireless unit parameters

for the programming of the wireless unit comprises causing the wireless unit to activate the wireless unit in the particular communications system.

21. A wireless unit that can be programmed over-the-air (OTA) by only a particular service provider, the wireless unit comprising:

a memory for storing a stored key relatively unique to the wireless unit and for storing wireless unit information;

a control for receipt of information OTA from the particular service provider;

a processor being functionally connected to the control and to the memory, and for, in response to the receipt of the information OTA from the particular service provider,

effecting generation of a trial verification number,

effecting comparison of the trial verification number with at least a portion of the information from the particular service provider for a match, and

in response to finding the match, effecting the storing of the information in the memory,

whereby the wireless unit can be programmed OTA only by the particular service provider that provides the information that results in the match with the trial verification number.

22. The wireless unit of Claim 21, wherein the stored key is generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm.

23. The wireless unit of Claim 22, wherein the identifier comprises an electronic serial number (ESN) of the wireless unit.

24. The wireless unit of Claim 22, wherein the stored key is generated by the wireless unit using the K-algorithm with the identifier associated with the wireless unit as the input to the K-algorithm.

25. The wireless unit of Claim 21, wherein the information comprises numeric assignment module (NAM) parameters.

26. The wireless unit of Claim 25, wherein the information comprises the NAM parameters and a verification number; and wherein the processor is operative to effect a comparison between the trial verification number and the verification number for the match.

27. The wireless unit of Claim 26, wherein the verification number is generated by an authorization algorithm (A-algorithm) having the NAM parameters and a key as A-algorithm inputs.

28. The wireless unit of Claim 27, wherein the key is generated by a key algorithm (K-algorithm) having an electronic serial number (ESN) associated with the wireless unit as a K-algorithm input.

29. The wireless unit of Claim 21, wherein the trial verification number is generated by using an authorization algorithm (A-algorithm) with the NAM parameters and the stored key as A-algorithm inputs.

30. The wireless unit of Claim 21, wherein the processor is operative, in response to failing to find the match, to block the storing of the information.

31. The wireless unit of Claim 21, wherein the programming comprises activation of the wireless unit in a particular communications system.